

日 本 国 特 許 庁
JAPAN PATENT OFFICE

19/1929-85
J1040 U.S. PTO
09/963261



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年10月 5日

出 願 番 号

Application Number:

特願2000-306420

出 願 人

Applicant(s):

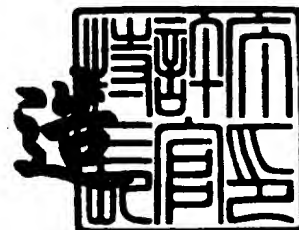
日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 8月31日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 49240046

【提出日】 平成12年10月 5日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/32

【発明者】

 【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

 【氏名】 森本 伸一

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100065385

 【弁理士】

 【氏名又は名称】 山下 穰平

 【電話番号】 03-3431-1831

【手数料の表示】

 【予納台帳番号】 010700

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9001713

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証拒否端末に対し特定条件でアクセスを許容する LAN

【特許請求の範囲】

【請求項 1】 LAN 内の基地局が、LAN 外からアクセスした端末局を認証して、認証を拒否された前記端末局に特定のサーバまたはネットワーク接続機器にアクセスを許容する LAN システムであって、

前記基地局は：

前記端末局と通信を行い、認証要求情報および受信パケットを抽出するインタフェース部と；

このインタフェース部からの前記認証要求情報を基に、LAN 内認証許可または拒否の判断を行い、その結果をパケット振り分けテーブルに設定する認証管理部と；

前記インタフェース部から送られたパケットを、前記パケット振り分けテーブルの登録内容を参照して、許可であれば当該端末局からのパケットを前記 LAN 内に配送し、拒否であれば前記特定のサーバまたはネットワーク接続機器に送信するパケット振り分け部とを有することを特徴とする LAN システム。

【請求項 2】 前記基地局が、第 2 の認証管理部と、第 2 のパケット振り分け部と、複数の振り分け先を格納した第 2 のパケット振り分けテーブルとを備え

前記第 2 の認証管理部は、前記認証管理部で拒否となった場合、前記認証要求情報を基に、認証許可または拒否の判断を行い、その結果を前記第 2 のパケット振り分けテーブルに設定し、

前記パケット振り分け部は、前記パケット振り分けテーブルの登録内容が認証拒否の場合、前記端末局からのパケットを前記第 2 のパケット振り分け部に転送し、

前記第 2 のパケット振り分け部は、前記第 2 のパケット振り分けテーブルの登録内容を参照して、前記端末局からのパケットを、その振り分け先に対応した特定のサーバまたはネットワーク接続機器に送信することを特徴とする請求項 1 記載の LAN システム。

【請求項 3】 前記認証管理部は、LAN 内認証サーバに対して認証要求を行い、その結果を前記パケット振り分けテーブルに設定することを特徴とする請求項 1 記載の LAN システム。

【請求項 4】 前記第 2 の認証管理部は、認証サーバに対して認証要求を行い、その結果を前記第 2 のパケット振り分けテーブルに設定することを特徴とする請求項 2 記載の LAN システム。

【請求項 5】 LAN 外からアクセスした端末局を認証して、認証を拒否された前記端末局に特定のサーバまたはネットワーク接続機器にアクセスを許容する LAN 基地局であって、

前記端末局と通信を行い、認証要求情報および受信パケットを抽出するインタフェース部と；

このインタフェース部からの前記認証要求情報を基に、LAN 内認証許可または拒否の判断を行い、その結果をパケット振り分けテーブルに設定する認証管理部と；

前記インタフェース部から送られたパケットを、前記パケット振り分けテーブルの登録内容を参照して、許可であれば当該端末局からのパケットを前記 LAN 内に配送し、拒否であれば前記特定のサーバまたはネットワーク接続機器に送信するパケット振り分け部とを有することを特徴とする LAN 基地局。

【請求項 6】 第 2 の認証管理部と、第 2 のパケット振り分け部と、複数の振り分け先を格納した第 2 のパケット振り分けテーブルとを備え、

前記第 2 の認証管理部は、前記認証管理部で拒否となった場合、前記認証要求情報を基に、認証許可または拒否の判断を行い、その結果を前記第 2 のパケット振り分けテーブルに設定し、

前記パケット振り分け部は、前記パケット振り分けテーブルの登録内容が認証拒否の場合、前記端末局からのパケットを前記第 2 のパケット振り分け部に転送し、

前記第 2 のパケット振り分け部は、前記第 2 のパケット振り分けテーブルの登録内容を参照して、前記端末局からのパケットを、その振り分け先に対応した特定のサーバまたはネットワーク接続機器に送信することを特徴とする請求項 5 記

載の L A N 基地局。

【請求項 7】 前記認証管理部は、L A N 内認証サーバに対して認証要求を行い、その結果を前記パケット振り分けテーブルに設定することを特徴とする請求項 5 記載の L A N 基地局。

【請求項 8】 前記第 2 の認証管理部は、認証サーバに対して認証要求を行い、その結果を前記第 2 のパケット振り分けテーブルに設定することを特徴とする請求項 6 記載の L A N 基地局。

【請求項 9】 L A N 外からアクセスして、認証を拒否された端末局に応答する L A N 基地局におけるパケット振り分け方法であって、

基地局が前記端末局から認証要求を受けて、L A N 内認証判断を行うステップと；

この認証判断結果が認証許可であれば、パケット振り分けテーブルに認証許可を登録し、認証拒否であれば、前記パケット振り分けテーブルに認証拒否を登録するステップと；

認証許可または拒否の登録後に前記端末局へ認証許可応答を行うステップと；

端末局からのパケットを受信して、前記パケット振り分けテーブルの当該端末局の認証登録状態を確認するステップと；

結果が認証許可であれば、当該パケットを L A N 内に配送し、認証拒否であれば、当該パケットを特定のサーバまたはネットワーク接続機器へ送信するステップを含むことを特徴とする L A N 基地局におけるパケット振り分け方法。

【請求項 1 0】 前記基地局が、複数の振り分け先を格納した第 2 のパケット振り分けテーブルを備え、

前記パケット振り分けテーブルの当該端末局の認証登録状態を確認して、認証拒否の場合、前記第 2 のパケット振り分けテーブルの登録内容を参照して、前記端末局からのパケットを、その振り分け先に対応した特定のサーバまたはネットワーク接続機器に送信するステップをさらに有することを特徴とする請求項 9 記載の L A N 基地局におけるパケット振り分け方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、特に無線ネットワークシステムに適用して好適な、LAN (Local Area Network) 内の基地局において、LAN 外からアクセスしてLAN 内認証拒否された端末局に対し、特定のサーバまたはネットワーク接続機器に対してのみアクセスを許容するLAN システムに関する。

【0002】

【従来の技術】

従来の無線ネットワークシステムの構成を第9図に示す。LAN 1 内の無線基地局 1 1 において、LAN 1 外の無線端末局 2 2 からの認証要求に対して、自局での認証またはLAN 内認証サーバ 1 2 に問い合わせを行い、その結果、LAN 内で認証許可されない無線端末局 2 2 に対しては、認証を拒否し、無線基地局内でパケットを廃棄していた。または、全ての無線端末を無条件に認証許可していた。

【0003】

例えば、特開平 1 1 - 2 0 5 3 8 8 号公報にて開示されたパケットフィルタ装置では、公衆網から直接私設網に接続する直結経路と、ファイアウォールを介して接続するファイアウォール経路とを設けておく。私設網から直結経路を介して受信したデータパケットは認証情報を付加して公衆網に送信し、ファイアウォール経路を介して受信したデータパケットはそのまま公衆網に送信する。また、公衆網から受信したデータパケットが、認証情報を付加されたデータパケットであれば、認証情報を取り除き、直結経路を介して当該データパケットを私設網に送信する。認証情報が付加されないデータパケットであれば、ファイアウォール経路を介して当該データパケットを送信する。

【0004】

【発明が解決しようとする課題】

しかしながら、従来の無線ネットワークシステムにおいては、次のような課題がある。すなわち認証登録されていない無線端末は、無線基地局経由でのLAN またはサーバへのアクセスを拒否されるため、会議などで無線基地局を使用する場合参加者全員の認証登録をその都度行う必要があった。また、無条件で認証許

可を行う方法もあるが、この場合無線基地局をLANへ接続するとセキュリティ上危険である等の問題があった。

【0005】

そこで本発明は、端末局のLANへの認証登録を行わなくとも、基地局にて特定のサーバやネットワーク接続機器への接続を許容し、ネットワーク管理者の負担軽減および端末局利用者の利便性を向上させることを課題とする。

【0006】

【課題を解決するための手段】

上述の課題を解決するため、本発明は、LAN内の基地局が、LAN外からアクセスした端末局を認証して、認証を拒否された前記端末局に特定のサーバまたはネットワーク接続機器にアクセスを許容するLANシステムであって、前記基地局は、前記端末局と通信を行い、認証要求情報および受信パケットを抽出するインタフェース部と、このインタフェース部からの前記認証要求情報を基に、LAN内認証許可または拒否の判断を行い、その結果をパケット振り分けテーブルに設定する認証管理部と、前記インタフェース部から送られたパケットを、前記パケット振り分けテーブルの登録内容を参照して、許可であれば当該端末局からのパケットを前記LAN内に配送し、拒否であれば前記特定のサーバまたはネットワーク接続機器に送信するパケット振り分け部とを有する。

【0007】

また、LAN外からアクセスした端末局を認証して、認証を拒否された前記端末局に特定のサーバまたはネットワーク接続機器にアクセスを許容するLAN基地局であって、前記端末局と通信を行い、認証要求情報および受信パケットを抽出するインタフェース部と、このインタフェース部からの前記認証要求情報を基に、LAN内認証許可または拒否の判断を行い、その結果をパケット振り分けテーブルに設定する認証管理部と、前記インタフェース部から送られたパケットを、前記パケット振り分けテーブルの登録内容を参照して、許可であれば当該端末局からのパケットを前記LAN内に配送し、拒否であれば前記特定のサーバまたはネットワーク接続機器に送信するパケット振り分け部とを有する。

【0008】

さらに、LAN外からアクセスして、認証を拒否された端末局に応答するLAN基地局におけるパケット振り分け方法であって、基地局が前記端末局から認証要求を受けて、LAN内認証判断を行うステップと、この認証判断結果が認証許可であれば、パケット振り分けテーブルに認証許可を登録し、認証拒否であれば、前記パケット振り分けテーブルに認証拒否を登録するステップと、認証許可または拒否の登録後に前記端末局へ認証許可応答を行うステップと、端末局からのパケットを受信して、前記パケット振り分けテーブルの当該端末局の認証登録状態を確認するステップと、結果が認証許可であれば、当該パケットをLAN内に配送し、認証拒否であれば、当該パケットを特定のサーバまたはネットワーク接続機器へ送信するステップとを含む。

【0009】

すなわち本発明は、LAN内の基地局において、そのLAN内で認証許可されない端末局に対しても基地局への接続を許可し、基地局では認証拒否された端末局から送信されたパケットに対してはパケット振り分けを行い、特定のサーバまたはネットワーク接続機器に対してのみアクセスを許容したことを特徴としている。

【0010】

【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して説明する。なお、以下の実施の形態では無線端末によるネットワークを例に説明するが、有線端末によるネットワークにおいても同様である。

【0011】

図1は、本発明の概略構成を示す。図において、LAN内の無線基地局11では、LAN外の無線端末局22からの認証要求に対して、無線基地局11内で認証判断し、またはLAN内アクセス許可端末情報を登録したLAN内認証サーバ12に問い合わせを行った結果、認証許可されない無線端末局22に対しても、無線基地局11との接続を許可する。認証拒否された無線端末局22から送信されたパケットに対しては、パケット振り分けを行い、特定のサーバ（またはゲートウェイ、ルータ等のネットワーク接続機器）13に対してのみアクセスを許容

する。無線基地局 1 1 とサーバ 1 3 は物理的に LAN への接続とは異なった専用線や、VPN (Virtual Private Network) 等 LAN を経由するが論理的に専用線となるような接続形態をとる。サーバ 1 3 の用途としては会議などで用いる資料や営業広告を保存するファイルサーバや、WWWサーバ等が考えられる。また、サーバ 1 3 は無線基地局 1 1 の内部に実装することも可能である。

【 0 0 1 2 】

無線基地局 1 1 を可搬型とし、各種イベント等に使用した場合等にイベントプログラム等を保存しておくこともでき、LAN へのアクセスはイベントスタッフだけが許可され、LAN への接続を拒否される観客はサーバのコンテンツを見るなどの利用が見込まれる。

【 0 0 1 3 】

次に図 2 を参照して、第 1 の実施形態における無線基地局の詳細な説明を行う。無線基地局 1 1 は、無線インタフェース部 1 1 1 と、認証管理部 1 1 2 およびパケット振り分けテーブル 1 1 4 と、パケット振り分け部 1 1 3 とで構成される。無線インタフェース部 1 1 1 は、無線端末局 2 1 および 2 2 と通信を行い、認証要求情報および受信パケットを抽出する。認証管理部 1 1 2 は、無線インタフェース部 1 1 1 からの認証要求情報を基に、内部認証テーブルでの認証判断または LAN 内認証サーバ 1 2 へ認証要求を行った結果により認証許可または拒否の判断を行い、その結果をパケット振り分けテーブル 1 1 4 へ設定を行う。パケット振り分け部 1 1 3 は、無線インタフェース部 1 1 1 から送られたパケットを、パケット振り分けテーブル 1 1 4 の登録内容を参照して、許可であれば当該無線端末局からのパケットを LAN 内に配送し、拒否であれば特定のサーバまたはゲートウェイ 1 3 に送信する。

【 0 0 1 4 】

図 3 は、パケット振り分けテーブル 1 1 4 の登録内容について示す。例えば無線端末を MAC (Media Access Control) アドレスで管理し、当該 MAC アドレスから送られたパケットは LAN 内へ配送する。また、パケット振り分けテーブル 1 1 4 は先に述べた自無線基地局内認証テーブルと同一として使用できる。

【 0 0 1 5 】

このようにして、本願発明では、LAN内で認証許可されない端末に対して、パケット振り分けを行い、特定のサーバ（プロキシサーバ等のファイアウォールを構成するものを含む）に対してのみアクセスを許容しているので、例えば社外からの訪問者に対しては無線基地局経由でISP (Internet Service Provider) に接続可能となる等、利便性を向上させることができる。また、特定のサーバに、営業宣伝等のコンテンツを入れておけば、商店街などに無線基地局を設置した場合に宣伝効果が得られる等の効果がある。

【 0 0 1 6 】

次に無線基地局 1 1 のパケット振り分け動作を図 4、5 に示すフローチャートを参照して説明する。図 4 は無線基地局 1 1 の認証管理部 1 1 2 の動作フローを示すもので、無線インタフェース部 1 1 1 から受け取った無線端末 2 2 からの認証要求が起点となり、パケット振り分けテーブル 1 1 4 への登録および無線端末局 2 2 への認証応答までを記載している。図 5 は無線基地局 1 1 のパケット振り分け部 1 1 3 の動作フローを示すもので、無線インタフェース部 1 1 1 から受け取った無線端末 2 2 からのパケット受信が起点となり、パケット振り分けテーブル 1 1 4 への確認およびパケットの振り分けまでを記載している。

【 0 0 1 7 】

図 4 において、無線端末局 2 2 から認証要求を受けると（ステップ 4 1）、無線基地局 1 1 は LAN 内認証サーバ 1 2 へ認証要求を行う（ステップ 4 2）。LAN 内認証サーバからの応答が認証許可であれば（ステップ 4 3）、パケット振り分けテーブルに認証許可を登録する（ステップ 4 4）。登録後、無線端末局へ認証許可応答を行う（ステップ 4 6）。LAN 内認証サーバからの応答が認証拒否であれば（ステップ 4 3）、パケット振り分けテーブルに認証拒否を登録する（ステップ 4 5）。登録後、無線端末局へ認証許可応答を行う（ステップ 4 6）。

【 0 0 1 8 】

図 5 において、無線端末局からパケットを受信すると（ステップ 5 1）、パケット振り分け部 1 1 3 はパケット振り分けテーブル 1 1 4 の当該無線端末局の認証登録状態を確認する（ステップ 5 2）。結果が認証許可であれば（ステップ 5

3)、当該パケットをLANへ送信する(ステップ54)。認証拒否であれば、当該パケットを特定のサーバまたはゲートウェイへ送信する(ステップ55)。

【0019】

次に本発明の第2の実施形態として、その基本構成は上記第1の実施形態と同様であるが、ISPと接続する場合について述べる。

【0020】

図6は、第2の実施形態における無線基地局の構成を示す。図において、LAN1に設置された無線基地局11において、無線端末局22からの認証要求に対して、自局での認証またはLAN内認証サーバ12に問い合わせを行った結果、LAN内で認証許可されない無線端末局22に対しても、無線基地局11との接続を許可するが、無線端末局22から送信されたパケットに対しては、パケット振り分けを行い、ファイアウォールを構成するサーバ13に対してのみアクセスを許容する。したがって、無線端末局22はサーバ13を経由し、無線端末局を登録しているISP網3のISPアクセスサーバに接続可能である。ISPアクセスサーバは無線端末局22の認証のため、ISP認証サーバ32に問い合わせを行い、認証許可であれば、接続を許可し、拒否であれば、接続を遮断する。

【0021】

次に第3の実施形態として、LANへの認証を許可されない無線端末局22からの送信パケットを、無線端末局22のユーザ情報から当該するISPへ接続するために、複数の接続先に振り分けることが可能となる場合について述べる。

【0022】

図7は、第3の実施形態の構成を示す。図2に示す第1の実施形態との相違点は、無線基地局11が、第2の認証管理部117と、第2のパケット振り分け部115と、複数の振り分け先を格納した第2のパケット振り分けテーブル116とを有する点である。無線インタフェース部111は、無線端末局21および22と通信を行い、認証要求情報および受信パケットを抽出する。認証管理部112は、無線インタフェース部111からの認証要求情報を基に、内部認証テーブルでの認証判断またはLAN内認証サーバ12へ認証要求を行った結果により認証許可または拒否の判断を行い、その結果をパケット振り分けテーブル114へ

設定を行う。認証管理部 1 1 2 が拒否判断を行った場合、第 2 の認証管理部 1 1 7 は、認証要求情報を基に、内部認証テーブルでの認証判断または外部認証サーバへ認証要求を行った結果により認証許可または拒否の判断を行い、その結果を第 2 のパケット振り分けテーブル 1 1 6 へ設定を行う。

【 0 0 2 3 】

パケット振り分け部 1 1 3 は、無線インタフェース部 1 1 1 から送られたパケットを、パケット振り分けテーブル 1 1 4 の登録内容を参照して、許可であれば当該無線端末局からのパケットを LAN 内に配送し、拒否であれば第 2 のパケット振り分け部 1 1 5 へ渡す。第 2 のパケット振り分け部 1 1 5 は、パケット到着時に第 2 のパケット振り分けテーブル 1 1 6 に振り分け先を確認し、その情報に従って特定のサーバまたはゲートウェイ 1 3 ~ 1 4 に送信する。

【 0 0 2 4 】

また、第 2 の認証管理部 1 1 7 を用いず、認証管理部 1 1 2 に、無線端末局 2 1, 2 2 のユーザデータ（ドメイン名や接続先 ISP 名等）を第 2 のパケット振り分けテーブル 1 1 6 に設定する機能を有することにより実現することもできる。

【 0 0 2 5 】

図 8 は、第 2 のパケット振り分けテーブル 1 1 6 の登録内容について示す。例えば各無線端末を MAC アドレスで管理し、振り分け先を併記する。

【 0 0 2 6 】

このように詳細に振り分けを行うことにより、複数の ISP に対して接続可能となり、ISP に接続できる無線端末局を増加させることができる。

【 0 0 2 7 】

【発明の効果】

以上説明したように、本発明は、LAN 外からアクセスした端末局が LAN 内で認証拒否されても、ゲートウェイ経由で ISP (Internet Service Provider) に接続可能なので、端末局利用者の利便性が高くなる。また、基地局設置者も、LAN への認証が拒否される不特定の端末局利用者に対して、特定のサーバのみへの接続を許可することにより、サーバ内に宣伝用コンテンツを保存しておくこ

とで、簡易に宣伝広告を行うことができるなどの利点がある。また、認証を拒否された端末局は強制的に特定のサーバまたはゲートウェイ等のネットワーク接続機器に接続されるので、LANのセキュリティも保つことができる。

【図面の簡単な説明】

【図 1】

本発明の概略構成を示す図である。

【図 2】

第 1 の実施形態における無線基地局の詳細構成を示す図である。

【図 3】

パケット振り分けテーブルの登録内容について示す図である。

【図 4】

無線基地局の認証管理部の動作を示すフローチャートである。

【図 5】

無線基地局のパケット振り分け部の動作を示すフローチャートである。

【図 6】

第 2 の実施形態における無線基地局の構成を示す図である。

【図 7】

第 3 の実施形態の構成を示す図である。

【図 8】

第 2 のパケット振り分けテーブルの登録内容について示す図である。

【図 9】

従来の無線ネットワークシステムの構成を示す図である。

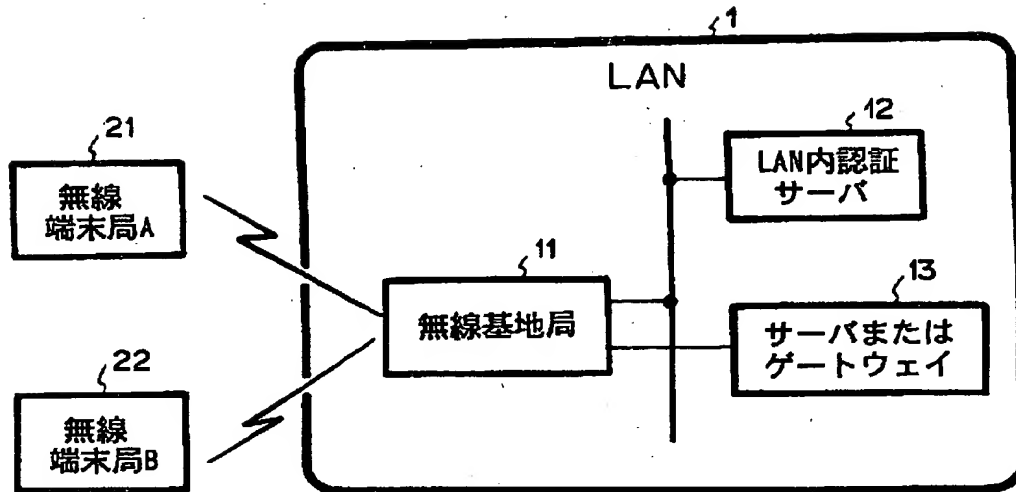
【符号の説明】

- 1 LAN
- 3 ISP (Internet Service Provider) 網
- 1 1 無線基地局
- 1 2 LAN 内認証サーバ
- 1 3 サーバまたはゲートウェイ
- 2 1 無線端末局 A

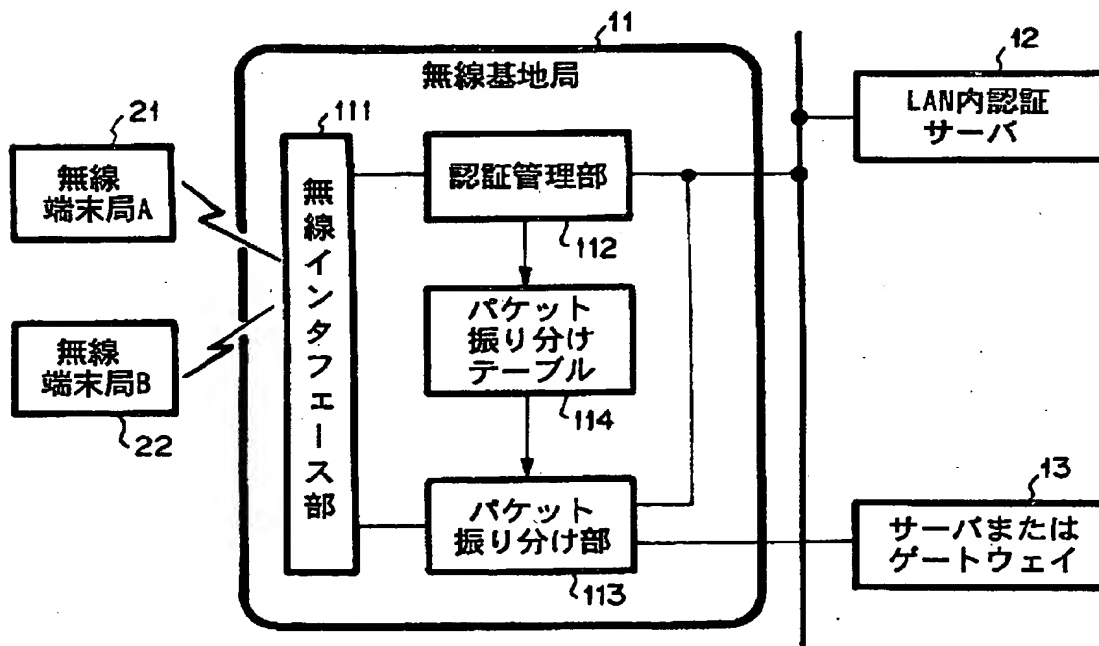
- 2 2 無線端末局 B
- 3 1 I S P アクセスサーバ
- 3 2 I S P 認証サーバ
- 1 1 1 無線インタフェース部
- 1 1 2 認証管理部
- 1 1 3 パケット振り分け部
- 1 1 4 パケット振り分けテーブル
- 1 1 5 第 2 のパケット振り分け部
- 1 1 6 第 2 のパケット振り分けテーブル
- 1 1 7 第 2 の認証管理部

【書類名】 図面

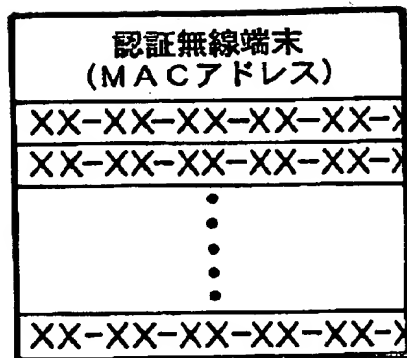
【図1】



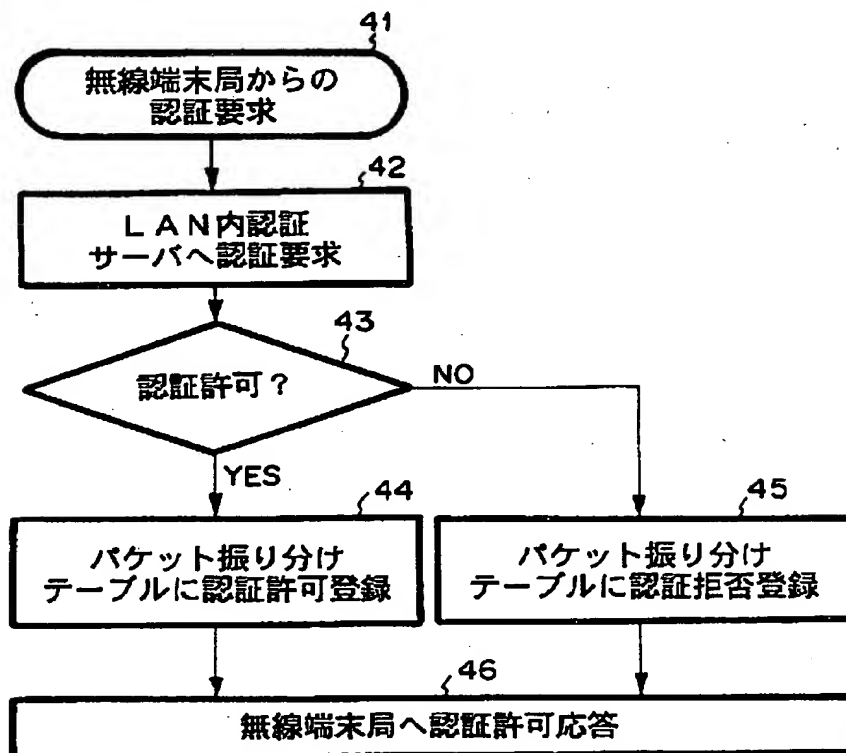
【図2】



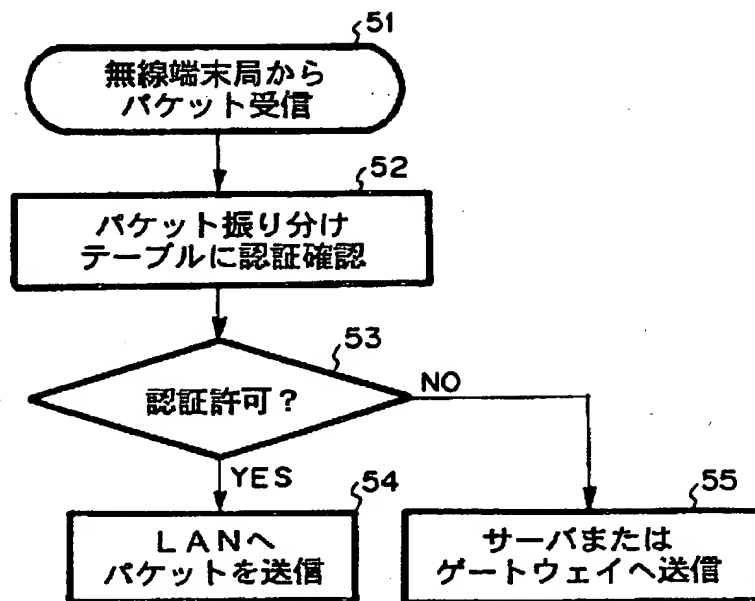
【図 3】



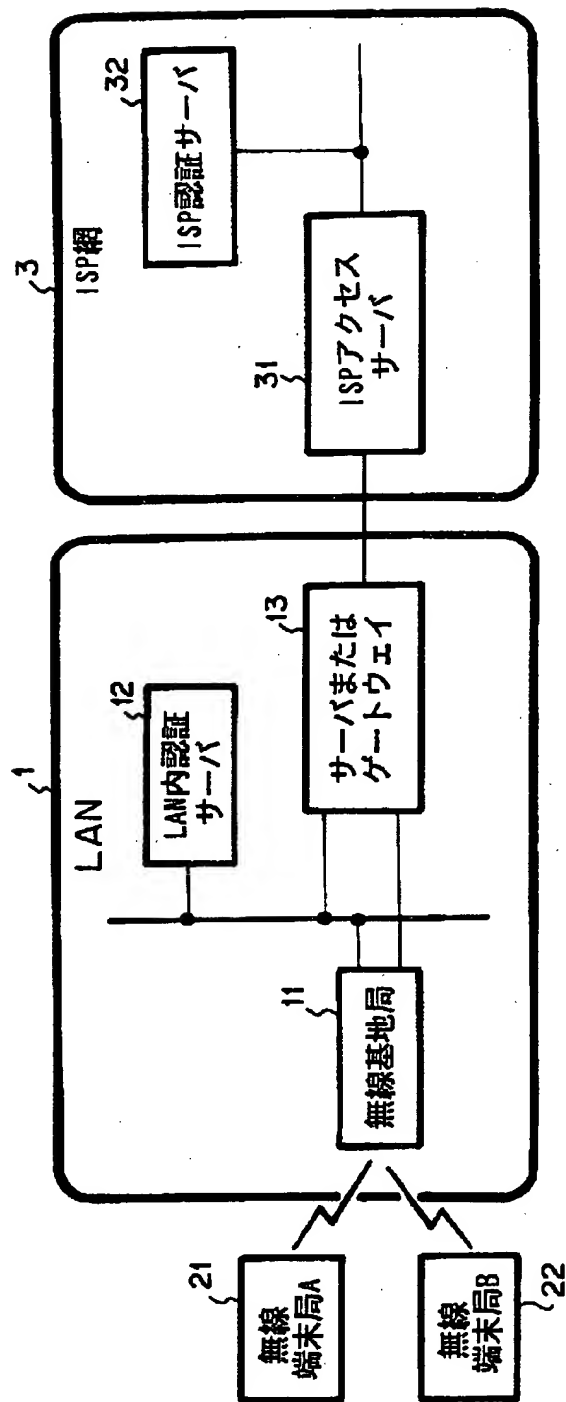
【図 4】



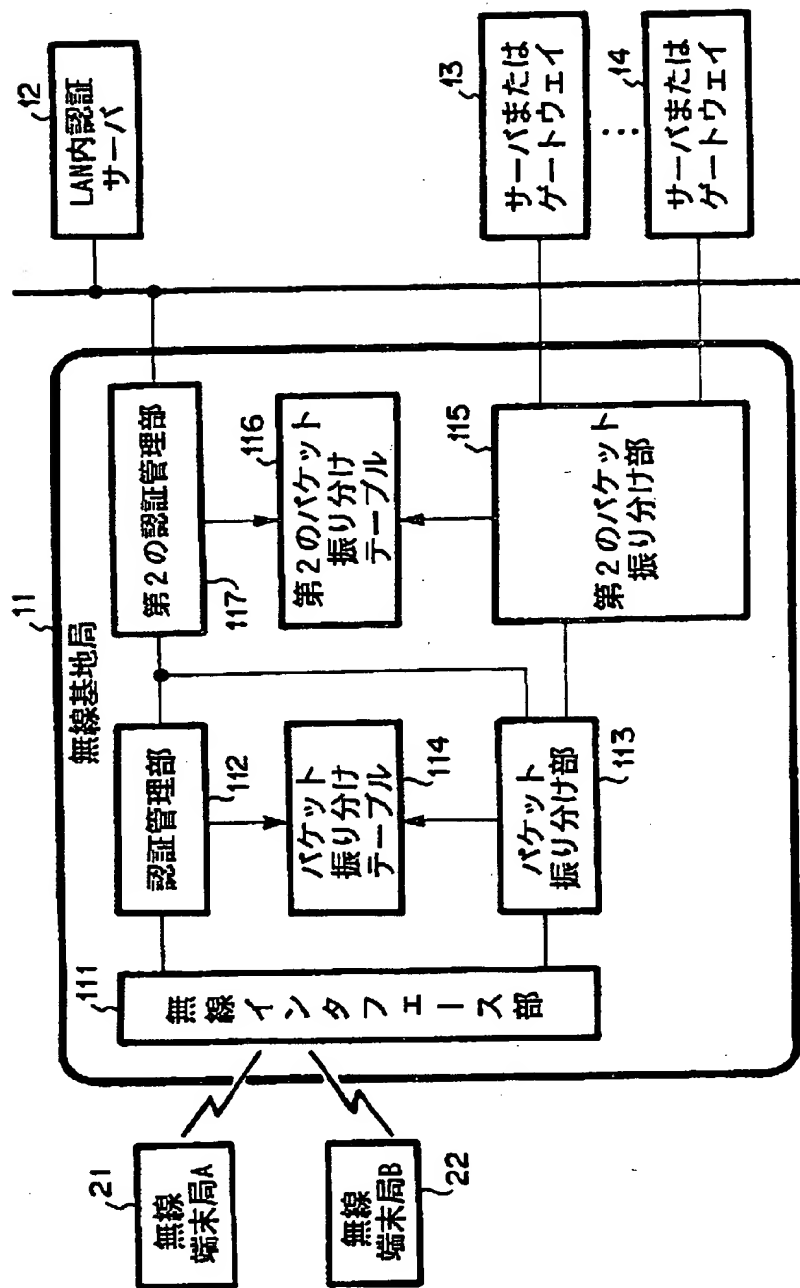
【図 5】



【図6】



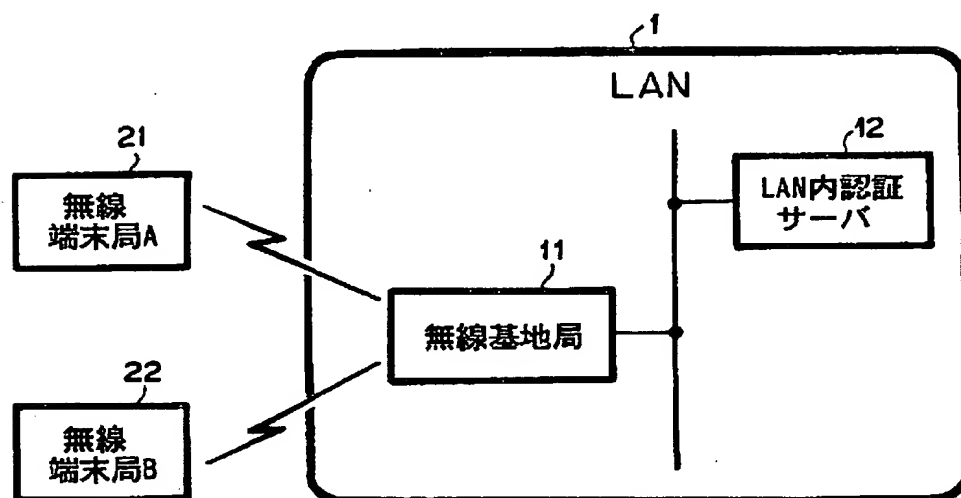
【図 7】



【図 8】

無線端末 (MACアドレス)	振り分け先
XX-XX-XX-XX-XX->	1
XX-XX-XX-XX-XX->	2
⋮	
XX-XX-XX-XX-XX->	n

【図 9】



【書類名】 要約書

【要約】

【課題】 LAN内の基地局において、LAN外からアクセスしてLAN内認証拒否された端末局に対しては、特定のサーバまたはネットワーク接続機器に対してのみアクセスを許容する。

【解決手段】 無線基地局11は、無線インタフェース部111にて、無線端末局21、22と通信を行い、認証要求情報および受信パケットを抽出する。認証管理部112では、認証要求情報を基に、LAN内認証許可または拒否の判断を行い、その結果をパケット振り分けテーブル114へ設定する。パケット振り分け部113では、受信パケットを、パケット振り分けテーブル114の登録内容を参照して、許可であれば当該無線端末局からのパケットをLAN内に配送し、拒否であれば特定のサーバまたはゲートウェイ13に送信する。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日
[変更理由] 新規登録
住 所 東京都港区芝五丁目7番1号
氏 名 日本電気株式会社